版权声明

本手册中的所有图片和产品规格参数仅供参考,随着软件或硬件的升级会略有差异，如有变更，恕不另行通知，如需了解更多产品信息，请浏览我们公司网站：http://www.tenda.com.cn。

目　　录

物品清单

小心打开包装盒，检查包装盒里是否有以下配件：

- TEI480T+/490T+/R6000+网吧/企业宽带路由器一台
- 一条电源线
- 一本用户手册
- 一张保修卡
- L 型支架两个
- 脚垫四个

⚠*注意：*

如果发现有所损坏或有任何配件短缺的情形，请及时与当地经销商联系。

第一章 产品概述

1.1 产品简介

感谢您购买本公司 TEI480T+/490T+/R6000+网吧/企业宽带路由器。TEI480T+/490T+/R6000+是 tenda 面向网吧/社区/企业/学校而设计的新一代多功能宽带接入产品。采用全球信赖的高品质、高稳定性的 Intel IXP 高端网络专用处理器，主频高达 533MHz，采用六层 PCB 专业设计，充分保证了整机性能强劲、稳定可靠。双向转发速率 200Mbps，可支持 70,000 多个联机数，封包处理快速稳定。强大的防火墙，有效防止各种黑客攻击、ARP 攻击与欺骗、ARP 病毒等等。

TEI480T+/490T+/R6000+除了包含所有宽带路由器常见功能外，还提供了诸多功能：客户机实时流量查看、基于 IP 的带宽控制、单机连接数控制、IP 与 MAC 绑定、UPnP、DDNS、VPN Pass-through、防火墙、管理型交换机等高级功能。

- 攻击防护功能：有效提高网吧的网络可靠性。支持 LAN 口和 WAN 口攻击防范，提供扫描类、DoS 类、可疑包和含有 IP 选项的包等攻击保护，能侦测及阻挡 IP 地址欺骗、源路由攻击、IP 与端口扫描、DoS 等网络攻击，有效防止 Nimda、冲击波、木马等病毒攻击，为网吧提供可靠的安全保障。
- 基于 IP、端口的 QoS：可限制单机带宽、连接数，有效防止用户使用 P2P 等特殊应用过度占用网络资源，让网络游戏更顺畅，并提供详细的流量统计列表。
- 支持 IP 与 MAC 绑定：有效防范 ARP 攻击。
- TEI480T+/490T+/R6000+提供双 WAN 口：采用特有的线路负载均衡

技术，可根据线路情况自动选择最优线路；不同 ISP 数据流选择对应 WAN 口线路传输；保证需通过相同 WAN 口传输的特殊应用(如部分游戏)顺利完成。

- 支持策略路由模式：自动分流电信、网通、铁通等多种网络供应商，保证以最快的速度到达。
- 支持端口镜像：便于网吧监控。网吧传输的数据可按要求复制到监控端口，满足公安部门的网吧监控要求，也为分析、解决网吧网络问题提供参考数据。
- 限制外网的 IP 及端口：保护局域网的安全。
- TEI480T+/490T+/R6000+提供全中文 Web 配置界面：配置简单，支持在线软件升级功能，全面满足网吧用户对高性能、多功能、高可靠性、高安全性的需求。

1.2 主要特性

- 符合 IEEE 802.3、IEEE 802.3u、IEEE 802.3x 等标准；
- 支持 PPPoE, PPP, IP, ARP, DHCP, TCP, UDP, HTTP, FTP, DNS 等协议；
- 提供 2 个 10/100M 自适应以太网（WAN）接口，可接 xDSL/以太网/Cable；
- 提供 3 个 10/100M 自适应以太网（LAN）接口，与内部局域网连接 ；
- 支持端口带宽控制、端口 VLAN 划分和端口镜像功能；
- 支持流量统计功能，可以分析整个网络的资源使用状况；
- 支持广域网物理参数的修改，满足用户特殊的需求；
- 支持 VPN Pass－through、UPnP 和 DDNS；
- 支持基于 IP 和端口的 QoS 设置，可限制单机带宽；

- 支持 IP 与 MAC 地址绑定，有效防范 ARP 攻击；
- 支持虚拟服务器、特殊应用程序、DMZ 主机和静态路由等功能；
- 支持连接数设置，可限制单机连接数；
- 支持广域网的带宽利用率显示，及时了解网络的带宽使用情况；
- 支持路由器访问控制，禁止非授权的 IP 地址访问路由器 WEB；
- 可根据线路情况自动选择最优线路；
- 不同 ISP 数据流选择对应 WAN 口线路传输；
- 保证需通过相同 WAN 口传输的特殊应用(如部分游戏)顺利完成；
- 内建防火墙，支持 IP 地址过滤、域名过滤、MAC 地址过滤；
- 提供攻击防护，可对网络攻击和病毒攻击进行防范；
- 可防止 DoS 攻击、能自动隔离带病毒的电脑，确保网络正常使用；
- 两条进线，出口带宽成倍增加，下载速度大大提高；
- 支持 MAC 地址修改和克隆，提供配置文件备份与载入；
- 限制外网的 IP 及端口，保护局域网的安全；
- 支持远程和 Web 管理，全中文配置界面，提供简易设置向导 ；
- 提供系统日志功能，支持外挂 Syslog 服务器记录信息；
- 提供详细的攻击、系统、安全日志；
- 支持线路检测功能，及时了解 ISP 线路情况；
- 内置电源，1U 钢壳，19 英寸标准机架结构，工业级设计；

1.3 产品规格

项目		规格
支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、ARP
端口	LAN 口	3 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
	WAN 口	2 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
	其它	1 个 Console 端口（RS232 DB9 公头）
网络介质		10Base-T：3 类或 3 类以上 UTP 100Base-TX：5 类 UTP
LED 指示	LAN/WAN 口	Link/Act（连接/工作） 100Mbps（速度）
	其它	Power（电源）、 SYS（系统状态指示灯）
外形尺寸（L x W x H）		294mm x 180mm x 44mm
使用环境		工作温度：0 C 到 40 C； 存储温度：-40 C 到 70 C； 工作湿度：10% 到 90% RH 不凝结； 存储湿度：5% 到 90% RH 不凝结
电源及功耗		输入：110-240VAC，50/60Hz（内部通用电源） 功耗：最大 5.2W

第二章 硬件描述

2.1 面板布置

2.1.1 前面板

1） Reset ：复位按钮。按住此按钮约 5 秒钟，路由器 SYS 系统状态灯将同时闪烁，此时松开复位按钮，路由器将恢复出厂设置并自动启动。

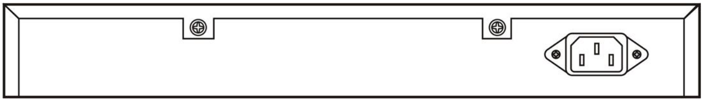
2） 指示灯：

指示灯	描 述	功 能
POWER	电源指示灯	供电正常，指示灯长亮
SYS	系统状态指示灯	闪烁表示系统正常 常亮或常灭表示系统不正常
Link/Act	广域网和局域网状态指示灯	常亮表示相应端口已正常连接 闪烁表示相应端口正在进行数据传输
100M	广域网和局域网速度指示灯	100M 灯常亮表示相应端口位于 100M 工作模式 100M 灯不亮表示相应端口位于 10M 工作模式

3） WAN：2 个广域网端口（RJ-45）。连接 xDSL Modem/Cable Modem 或以太网。

4） 局域网端口：3 个 RJ-45 接口。计算机、HUB 和交换机通过这些端口连接局域网。

2.1.2 后面板



电源：使用专用配置电源。

2.2 系统需求

- 64M以上内存
- 200Mhz以上处理器
- 10M网络适配器以上
- Internet Explorer 5.0或更高版本
- 宽带Internet服务(接入方式为通过xDSL/Cable Modem/以太网接入)

2.3 安装环境

2.3.1 安装环境要求

- 将设备水平放置
- 设备勿用湿布擦拭
- 尽量使设备远离发热器件
- 将设备置于清洁干燥的环境
- 雷雨天气请将设备电源及所有连接拆除，以免遭雷击破坏

2.3.2 推荐使用环境

- 温度：0℃∽40℃
- 湿度：10％∽90％ＲＨ(非雾水)

2.4 硬件安装步骤

在安装路由器前,我们希望您已经能够利用您的宽带服务在单台计算机上成功上网，如果您单台计算机上宽带网有问题，请先和您的网络供应商（ISP）联系解决问题，当您成功地利用单台计算机上网后，请遵循以下步骤安装路由器。

- **建立局域网连接**

  将路由器 LAN 口和局域网中的 Hub 或交换机连接。您也可以将路由器 LAN 口直接和您的计算机网卡连接。
- **建立广域网连接**

  将 xDSL 或以太网接入五类线和路由器 WAN 口相连。
- **连接电源**

  将电源连接好，路由器将自行启动。

第三章 快速安装

3.1 计算机配置

路由器默认 IP 地址是：192.168.0.1，可根据您的需要进行改变，但是我们在这本用户手册上将按照默认值进行设置。

将您的计算机连接到路由器的 LAN 口，并按照下面步骤进行设置：

➢ 在您正在使用的桌面上，用右键单击“网上邻居”，在弹出的菜单中选择“属性”；



➢ 在随后打开的窗口里，用鼠标右键点击“本地连接”，选择“属性”；

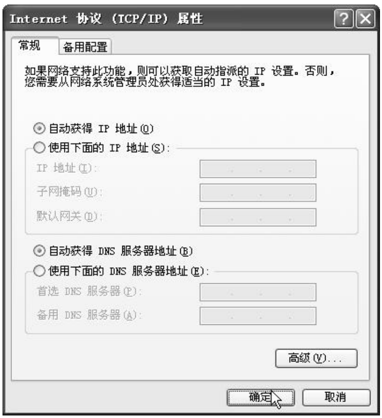


- 在弹出的对话框里，先选择“Internet 协议（TCP/IP)”，再用鼠标点击“属性”按钮；



- 在随后打开的窗口里，您可以选择“自动获得 IP 地址（O)”或者是“使用下面的 IP 地址（S)”；

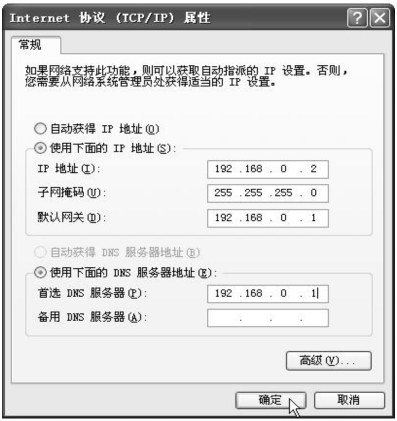
  “自动获得 IP 地址（O)”、“使用下面的 IP 地址（S)”如图：



注意:

设置您计算机的 IP 地址为 192.168.0.XXX(XXX 为 2~254)，子网掩码：255.255.255.0，网关： 192.168.0.1，DNS 服务器：您可以填写您当地的 DNS 服务器地址（可咨询您的 ISP 供应商）也可以由路由器作为 DNS 代理服务器。

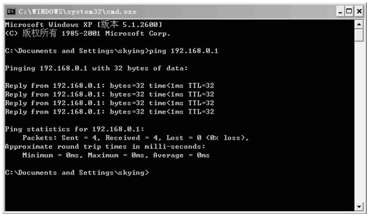
设置完成后点击“确定”提交设置，再在本地连接“属性”中点击“确定”保存设置。



3.2 验证连通性

设置好 TCP/IP 参数后，您可以使用 Ping 命令检查您的计算机和路由器之间是否连通：

- 选择“开始——运行”在运行对话框输入“cmd”点确定。
- 按图格式输入“ping 192.168.0.1”并回车，如能得到图示的回应，则表明您的计算机与路由器连接正常。否则请检查路由器是否通电，计算机到路由器的网线是否连接好。



3.3 快速安装

本产品提供基于浏览器的配置界面、这种配置方式同样适合任何 MS Windows、Macintosh 或 UNIX 平台。

打开浏览器，在地址栏中键入“http://192.168.0.1”，并回车；



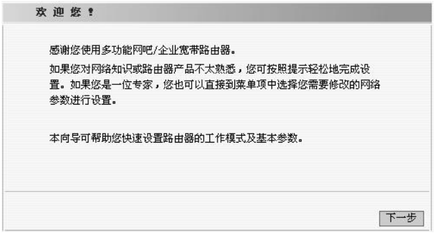
连接建立后，您会看到登录界面。您需要以系统管理员的身份登录，输入用户名和密码（用户名和密码出厂设置均为“admin”），为下次快速进入路由器管理页面请选择记住我的密码。

⚠*注意：*

为了路由器的安全，请正确登录后修改系统默认的用户名和密码！



如果您输入的用户名和密码正确，浏览器将进入管理员模式的画面，并出现一个快速设置向导，点击“下一步”，进入上网方式选择画面。

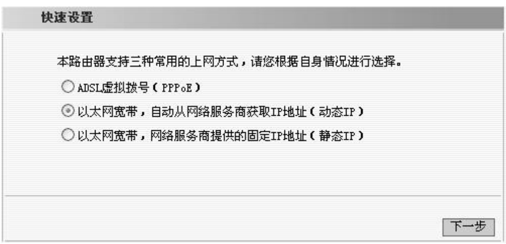


选择您需要设置的 WAN 口数，并点击下一步进行设置。



本路由器支持最常见的三种上网方式，（路由器的默认接入方式为动态 IP 接入）：

- PPPOE 拨号上网（ADSL）：采用 PPPOE 虚拟拨号来进行 Internet 连接。
- 动态 IP：宽带网络或者有线通（例如：长城宽带）通过 DHCP 服务为用户分配 IP 地址。
- 静态 IP：以太网宽带接入方式，ISP（例如：长城宽带）提供的固定 IP 地址。



可根据自身情况进行选择，然后单击“下一步”填写上网所需的基本网络参数。

3.3.1 PPPOE

如果您的上网方式为“ADSL 虚拟拨号”，只需要在“用户名”及“密码”中输入框中输入 ISP 服务商提供给您的帐号信息。



- 上网帐号：填入 ISP 为您指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- 上网密码：填入 ISP 为您指定的 ADSL 上网密码，不清楚可以向 ISP 询问。

3.3.2 动态 IP

如果您的上网方式为“动态 IP”，通过此种接入，您可以从 ISP 服务商处动态获取到 IP 地址访问 Internet；不需其它设置，点击“下一步”保存即可。

⚠*注意：*

路由器 WAN 口获取的 IP 地址和路由器 LAN 口 IP 地址在同一网段，将会影响路由器的使用，导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

3.3.3 静态 IP

如果您的上网方式为“静态 IP”，输入 ISP 提供给您的固定 IP 地址，子网掩码，网关地址以及主 DNS、备用 DNS 地址；点击“下一步”保存即可。

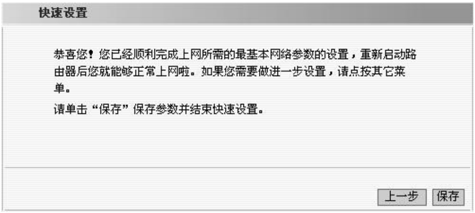


- IP 地址：本路由器对广域网的 IP 地址，即 ISP 提供给您的 IP 地址，不清楚可以向 ISP 询问。
- 子网掩码：本路由器对广域网的子网掩码，即 ISP 提供给您的子网掩码，不清楚可以向 ISP 询问。
- 网关：填入 ISP 提供给您的网关，不清楚可以向 ISP 询问。
- DNS 服务器：填入 ISP 提供给您的 DNS 服务器，不清楚可以向 ISP 询问。
- 备用 DNS 服务器：可选，如果 ISP 提供两个 DNS 服务器地址，您可以将另一个 DNS 服务器地址填入此处。

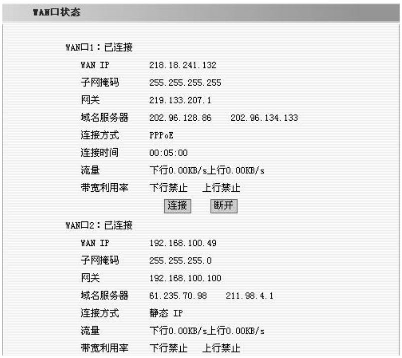
⚠*注意：*

路由器 WAN 口指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，将会影响路由器的使用，导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

在填写完上网的基本网络参数后，您可来到设置向导的完成画面。



当设置完成以后可以到“运行状态”中“WAN 口状态”中查看配置信息。



第四章 配置说明

4.1 启动和登录

在启动和登录成功以后，浏览器会显示管理员模式的画面。在左侧菜单栏中，共有“运行状态”、“快速设置”、“局域网设置”、“广域网设置”、“DHCP 服务器”、“双 WAN 口设置”、“虚拟服务器”、“安全设置”、“QOS 设置”、“连接数设置”、“IP 与 MAC 绑定”、“流量统计”、“交换功能设置”、“路由设置”、“动态 DNS”、“系统工具”、“系统日志”、“退出登录”十八个菜单。单击某个菜单项，您即可进行相应的功能设置。



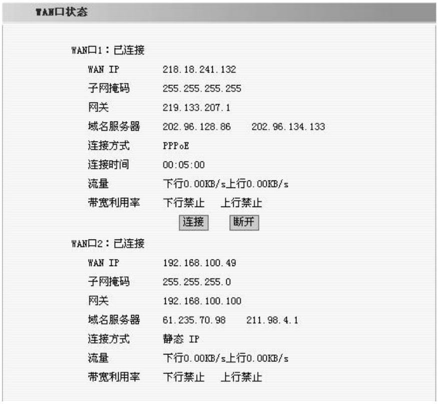
在使用过程中，如果您对本产品的功能有任何问题，您只需单击该页面的“帮助”按钮，即可获得详细的联机帮助。

下面将详细讲解各个菜单的功能。

4.2 运行状态

4.2.1 WAN 口状态

此处显示当前 WAN 口连接状态、WAN IP、子网掩码、网关、域名服务器、备用域名服务器、WAN 口流量、带宽利用率、连接方式。



- WAN 口连接状态：显示 WAN 口的连接状态。

  未连接：表示 WAN 口未接网线；

  连接中：表示 WAN 口已接通，正在获取 IP 地址；

  已连接：表示路由器与 ISP 已正常接通；
- WAN IP：从 ISP 获取的 IP 地址。
- 子网掩码：从 ISP 获取的子网掩码。
- 网关：从 ISP 获取的网关。
- 域名服务器：从 ISP 获取的域名服务器。
- 备用域名服务器：从 ISP 获取的备用域名服务器。
- WAN 口流量：表示当前路由器已使用的带宽，单位为 KB/S。

例如：ISP 分配的带宽为 2Mb/s=256KB/s=2048Kb/s

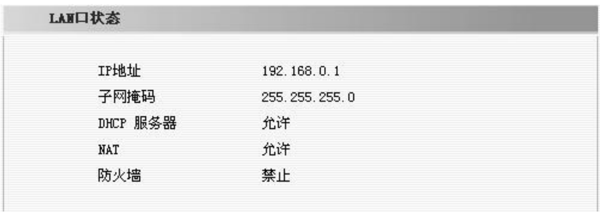
- 带宽利用率：已使用实际的总带宽的百分比。

  实际的总带宽请在 QOS 设置中进行设置，只有启用 QOS 规则后，此功能才会生效，否则禁止。QOS 设置总带宽时一定要填写准确，否则带宽利用率会超过 100%。

- 连接方式：表示当前您选的接入方式。

4.2.2 LAN 口状态

此处显示当前路由器的 IP 地址、子网掩码和 DHCP 服务、NAT、防火墙的基本情况。



- IP 地址：显示当前路由器的 IP 地址；
- 子网掩码：显示当前路由器子网掩码；
- DHCP 服务：显示 DHCP 服务器开启和关闭状态，此处和页面中的“DHCP 服务器”→“DHCP 服务器设置”相对应；
- NAT：显示路由器的工作模式；
- 防火墙：显示当前防火墙的状态；默认为禁止，只有当用户设置“安全 设置”中的“客户端过滤”、“URL 过滤”、“MAC 地址过滤”中的任何一项，运行状态中的“防火墙”状态将会变允许。

4.2.3 信息

显示路由器当前运行时间、系统时间、已连接客户端数，NAT 连接数、系统版本、引导程序版本、LAN 口 MAC 地址、WAN 口 MAC 地址、硬件版本号等信息。



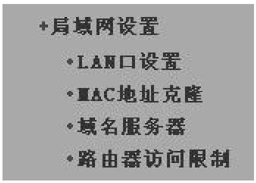
- 运行时间：显示系统正常启动后的运行时间；
- 系统时间：显示系统更新时间；
- 已连接客户端数：显示已连接的计算机数；
- NAT 连接数：显示路由器已使用的 NAT 数；
- 系统版本：显示路由器的软件版本；
- 引导程序版本：显示路由器的程序版本；
- LAN 口 MAC 地址：显示路由器 LAN 口 MAC 地址；
- WAN 口 1 MAC 地址：显示路由器 WAN 口 1 MAC 地址；
- WAN 口 2 MAC 地址：显示路由器 WAN 口 2 MAC 地址；
- 硬件版本号：显示路由器的硬件版本；

4.3 设置向导

请参照第三章的快速安装。

4.4 局域网设置

在“局域网设置”菜单下面，共有“LAN 口设置”、“MAC 地址克隆”和“域名服务器”“路由器访问限制”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。



4.4.1 LAN 口设置



- IP 地址：本路由器对局域网的 IP 地址。该 IP 地址的出厂设置为 192.168.0.1，您可以根据需要改变它。
- 子网掩码：本路由器对局域网中的子网掩码，可手动输入。

⚠*注意:*

如果您改变了本 IP 地址，您必须用新的 IP 地址才能登录路由器进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置为该 IP 地址才能正常上网。

路由器 WAN 口获取或指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，将会影响路由器的使用，导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

4.4.2 MAC 地址克隆



某些 ISP 服务商会绑定用户计算机的 MAC 地址，请将当前管理者使用的计算机的 MAC 地址复制到 WAN 口 MAC 地址中或手动更改 MAC 地址。修改此值后，运行状态中的 WAN 口 MAC 地址将会改变。

- MAC 地址：默认显示路由器 WAN 口 MAC 地址，可手动输入 MAC 地址。
- 恢复出厂 MAC：点击后 MAC 地址栏会显示路由器出厂 MAC 地址。
- 克隆 MAC 地址：点击后 MAC 地址栏会显示当前计算机的 MAC 地址。

⚠注意：

修改 WAN 口 MAC 地址后，需重新启动路由器才会生效，如 ISP 不绑定您的路由器的 MAC 地址，请不要使用此功能，以免出现其它问题。

4.4.3 域名服务器



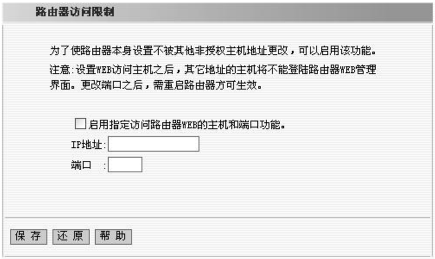
- 域名服务设置：默认为关闭，启动后，计算机将获取到下面填写的 DNS 服务器地址；
- 域名服务代理：默认启用，将路由器的 IP 地址做为 DNS 服务器地址分配给计算机。
- DNS 服务器：填入 ISP 提供给您的 DNS 服务器，不清楚可以向 ISP 询问。
- 备用域名服务器：可选项，如果 ISP 提供给您四个 DNS 服务器，则您可以把另三个 DNS 服务器的地址填于此处。此处和“DHCP 服务器设置”中的备用域名服务器地址相同，但只能修改此处的参数系统才会生效。如修改“DHCP 服务器设置” 中的备用域名服务器地址，系统将不做保存处理。

⚠*注意:*

DNS 的主要作用是把我们输入的域名（网址）解析为 IP 地址。

4.4.4 路由器访问限制

为了增加路由器管理的安全性，您可以指定计算机的 IP 地址和更改路由器端口号来进行管理。



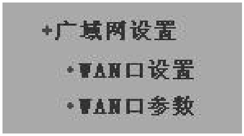
- 启用：开启访问路由器 WEB 限制功能。
- IP 地址：输入局域网中计算机的 IP 地址。
- 端口：默认端口为 80，输入您访问路由器 WEB 界面的端口号。

⚠*注意：*

设置指定 IP 地址之后，其它地址的主机将不能登陆路由器 WEB 界面。当修改访问路由器的端口时，路由器需重新启动。例如：路由器的地址为 192.168.0.1，IP 地址为 192.168.0.1，访问端口改为：8888，则登陆路由器的管理页面是：192.168.0.1:8888

4.5 广域网设置

在“广域网设置”菜单下面，共有“WAN 口设置”、“WAN 口参数”二个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。



4.5.1 WAN 口设置

根据您选择的设置的 WAN 口及 WAN 口的连接类型，即您的上网方式，可做相应的修改。本路由器默认的上网方式为“动态 IP”。

4.5.1.1 动态 IP

如果您的上网方式为动态 IP，即您可以自动从网络服务商（例如：中国电信、长城宽带）获取 IP 地址。



- MTU 默认值为 1500，请根据实际情况进行修改。

4.5.1.2 静态 IP

如果您的上网方式为静态 IP，即您拥有网络服务商（例如：中国电信、中国网通）提供的固定 IP 地址，MTU 默认值为 1500。



➢ MTU 默认值为 1500，请根据实际情况进行修改。

4.5.1.3 PPPOE

如果您的上网方式为 ADSL 虚拟拨号方式，在该页面您可以更改、设置其它参数。



- 上网帐号：也就是您的上网帐号，填入 ISP 为您指定的 ADSL 上网帐号。
- 上网口令：填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。
- 服务名称：填入 ISP 为您提供的登陆服务名称。（可选）
- MTU：默认值为 1492，可根据您的需要进行修改，MTU 值最大不能超过 1492。
- 自动连接：在开机和断线后自动进行连接。
- 手动连接：由用户手动进行连接。
- 按需连接，在有访问数据时自动进行连接。
- 定时连接，在指定的时段自动进行连接。

4.5.2 WAN 口参数

该页面提供端口状态、端口流量控制、端口速率等设置，您可以按照下面说明正确设置参数。



4.5.2.1 WAN 口状态表

该项用来设置并显示 WAN 口的状态信息。

- 端口状态：您可以进行需要设置 WAN 口的状态，启用和禁用。
- 流量控制：启用表示对该端口的数据流量控制，反之则不加控制。
- 协商模式：您可以进行需要设置 WAN 口的协商模式：自协商、10M 半双工、10M 全双工、100M 半双工、10M 全双工。

	端口状态	流量控制	协商模式
WAN1	启用	启用	自协商
WAN2	启用	启用	自协商

4.5.2.2 协商状态表

该项用来显示端口的协商状态信息。

- 端口状态：显示端口的连接状态。即是否已经连接上。
- 连接速率：显示端口连接的实际速率。
- 双工模式：显示端口通信采用的双工模式：全双工或半双工。
- 流量控制：显示端口是否启用了流量控制。

协商状态	端口状态	连接速率(Mbps)	双工模式	流量控制
WAN1	已连接	100	全双工	启用
WAN2	已连接	100	全双工	启用

4.5.2.3 端口限制信息表

该项用来设置并显示端口的各种限制信息。

- 入口限制模式:该项用来选择对进入该 WAN 口的数据包采用的限制类型：所有帧、FLOOD、广播和多播、广播和不限制。
- 入口限制速率：该项用来选择对进入该 WAN 口数据包速率，其中可以选项有 128Kbps、256Kbps、512Kbps、1MKbps、2MKbps、4MKbps、8MKbps。
- 出口限制：选中该复选框表示启用出口限制，即对该 WAN 口转发的数据包进行控制，反之则不启用。
- 出口限制速率：该项用来限制从该 WAN 口转发的数据包速率，其中可选项有 128Kbps、256Kbps、512Kbps、1MKbps、2MKbps、4MKbps、8MKbps。



4.6 DHCP 服务器

在“DHCP 服务器”菜单下面，有“DHCP 服务器设置”、“DHCP 客户端列表”、“静态地址分配”三个子项。下面将详细讲解各子项的功能。



4.6.1 DHCP 服务器设置

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、以及 DNS 服务器等。为您局域网中所有的计算机正确配置 TCP/IP 协议并不是一件容易的事，幸运的是，DHCP 服务器提供了这种功能。如果您使用本路由器的 DHCP 服务器功能的话，您可以让 DHCP 服务器自动替您配置局域网中各计算机的 TCP/IP 协议。



- DHCP 服务器：如果您想使用 DHCP 的自动配置 TCP/IP 参数功能，请启动该选项。

- 地址池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。
- 地址池结束地址：DHCP 服务器所自动分配的 IP 的结束地址。
- 地址租期：DHCP 服务器分配的 IP 地址租期，默认为 1440 分钟。
- 主 DNS 服务器和备用 DNS 服务器：此值随“局域网设置”→“域名服务器设置”中的主 DNS 服务器和备用 DNS 服务器变化而变化，如您需要更改此值，请到“局域网设置”→“域名服务器设置”页面中进行更改。

⚠ *注意：*

为了使用本路由器的 DHCP 服务器功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”。

4.6.2 DHCP 客户列表

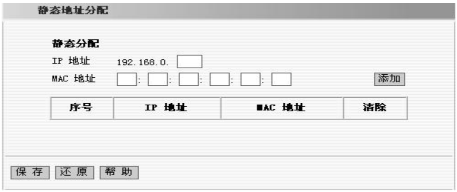
该客户列表显示了所有通过 DHCP 获得 IP 的主机名、IP 地址、MAC 地址、租约时间等等



- 主机名：客户端的主机名。
- IP 地址：客户端申请到的 IP 地址。
- MAC 地址：申请到该 IP 地址的计算机的 MAC 地址。
- 租约时间：主机通过 DHCP 所获得的 IP 的使用时间。

4.6.3 静态地址分配

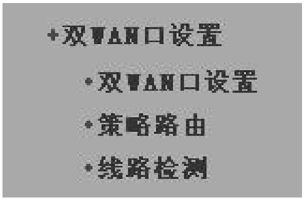
为了方便您对局域网中的计算机 IP 地址进行控制、本路由器内置了静态地址分配功能,该功能可以为具有指定 MAC 地址的计算机保留静态的 IP 地址，之后，此计算机请求 DHCP 服务器获得 IP 地址时，DHCP 服务器将给它分配此预留的 IP 地址。



- MAC 地址：预留 IP 地址的计算机的 MAC 地址。
- IP 地址：预留的 IP 地址。
- 添加：将预留的 IP 地址和 MAC 地址添加到表中。
- 清除：将已建立的静态分配信息清除。

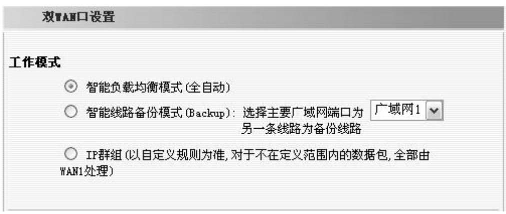
4.7 双 WAN 口设置

在“双 WAN 口设置”菜单下面，有“双 WAN 口设置”、“策略路由”和“线路检测”三个子项。单击某个子项，您即可进行相应的功能查看与设置。



4.7.1 双 WAN 口设置

4.7.1.1 工作模式



本路由器提供三种负载均衡机制：

➢ 智能负载均衡模式(全自动)：当您选用智能负载均衡模式，路由器将以联机数并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。线路的带宽是依据您所填入的频宽设定，例如当两条

广域网都为上行512Kbit/sec 时，其自动负载比例为1:1，当一条线路的上行带宽为1024kbit/sec 另一条为512kbit/sec 时，则此自动负载比例为2:1，所以为了确保你的路由器达到实际线路负载能够均衡，请填入实际上行下载带宽。

- ➢ 智能线路备份模式(Backup)： 选择主要广域网端口，另一条线路为备份线路。当您选择此模式时，局域网计算机的所有数据将从主WAN 口出去，如主 WAN 口线路问题，则自动切换到备份线路，不会出现掉线情况。
- ➢ IP 群组(以自定义规则为准，对于不在定义范围内的数据包，全部由 WAN1 处理)。当您选择此模式时，用户自定义负载设置优先，对于不在范围的数据包全部由 WAN1 处理，如出现 WAN1 线路问题，则自动切换到 WAN2。

不论是智能负载均衡或是智能线路备份模式、还是IP群组模式，搭配“用户自定义负载设置”可以有更弹性运用您的带宽，您可将特定的内网IP，使用特定应用服务作访问，或特定的目的地IP经由您指定的广域网来访问外网。

4.7.1.2 ISP 线路设置

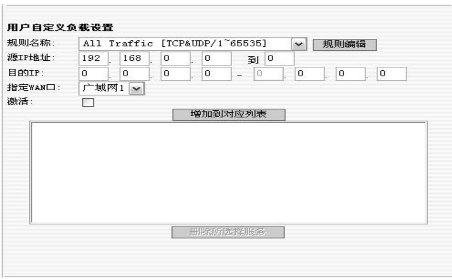


TEI480T+/490T+/R6000+路由器会依照您实际输入的上传带宽数据做为两条广域端口自动负载平衡的比例依据。例如当两条广域网都为上传512Kbit/sec 时，其自动负载比例为1：1。当一条线路的上传频宽为

1024kbit/sec 另一条为512kbit/sec 时，则此自动负载比例为2：1。所以为了确保您的路由器达到实际线路负载能够均衡，请填入实际上行下行带宽。

4.7.1.3 自定义

使用者可将特定的IP或特定的应用服务端口(Service port)经由您限定的WAN出去。其它没有做绑定的IP或Service还是会进行广域网的负载平衡。



- 规则名称：在此选择欲开启的绑定服务端口，从下拉式选单中可以选择预设列表(如All-TCP&UDP 0∽65535，WWW为80∽80，FTP为21∽21等等)，默认显示为All 0∽65535。
- 源IP地址：指定局域网中的IP地址的计算机的数据包指定从哪个WAN口出去。在此填上局域网IP地址范围，例如192.168.0.10到100。
- 目的IP：指定局域网中的IP地址的计算机的数据包指定从哪个WAN口出去，并从哪个WAN口去访问广域网指定的IP地址。如果您知道某个游戏服务器的地址，您可以指定WAN口最快的线路去访问。若只需要设定特定的应用而不需指定特定的IP地址，则在IP的字段皆填入0.0.0.0。

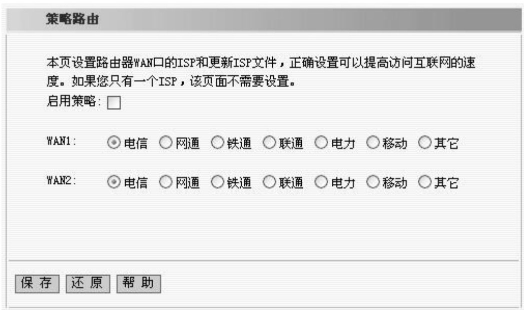
- 指定WAN口：指定局域网的数据从哪个WAN口出去。
- 激活：启用此规则。
- 增加到对应列表： 增加此条规则到列表。
- 删除所选服务： 删除在服务列表里所选择的规则。
- 规则编辑：按下此按钮可以进入规则设定页面，在此页面可以新增或删除的服务端口。



- 服务端口名称： 在此自定义开启的服务规则名称，如BT等。
- 通讯协议：在此选择欲开启的服务规则的封包格式为TCP或UDP。
- 服务端口的位置范围： 将你所需新增加的服务端口范围填入。
- 增加到对应列表： 增加到开启服务项目内容列表，最多可新增100组。
- 删除所选服务端口列表：删除所选择的开启服务项目之一的内容。
- 确定：按下此按钮“确定”即会储存刚才所变动的修改设定内容参数。
- 取消：按下此按钮“取消”即会清除刚才所变动的修改设定内容参数。
- 离开：离开此功能设定画面。

4.7.2 策略路由

该页主要设置路由器的 WAN 口 ISP 类型，正确设置该项可以实现针对不同 ISP 的所有数据包的自动分流，从而提高访问互联网的速度，如果您申请的两条线路都是同一个 ISP 提供的，则该页面不需要设置，下面将详细说明此功能。



- 当您启用策略路由模式时，您只需要根据您实际的ISP线路进行选择即可，路由器会依照内建的策略自动分流。真正实现“电信走电信，网通走网通”及其它分流策略。
- 启用策略：选择是否启用策略路由器，只有启用后，该项的设置才能生效。
- WAN1：选择您WAN1对应的ISP类型。
- WAN2：选择您WAN2对应的ISP类型。

4.7.3 线路检测

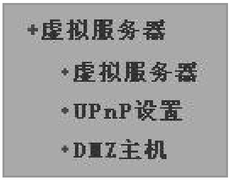
当使用两条广域网线路时，可启用此功能，以避免因为广域端口流量过大时造成路由器的误判将此线路判断为断线，路由器根据用户的设置自动进行线路检测。



- 重新发起测试次数：对外联机侦测重试次数，默认值为五次。若是于此设定次数当中，Internet没有回应的话，就判断为对外线路中断！
- 响应延迟时间：对外联机侦测时间（秒），默认值为30秒。根据设定秒数之后重新测试对外联机。
- 线路侦测机制：当侦测到与ISP连接失败时，系统就会在系统日志中将这项错误讯息纪录下来，但依旧保持此线路不会移除。
- 预设网关：就是路由器获取到外网IP地址的网关。
- ISP服务器：填入ISP的DNS服务器等。在设定此IP地址时请确认此IP地址是可以且稳定快速的得到响应。
- 远程服务器：远程的网络节点侦测位置，此地址最好也是可以且稳定快速的得到响应（建议填入ISP端DNS IP）。
- 使用DNS服务器做域名解释：此字段只填入网址 如“www.163.com”，（请勿填IP地址）。另外，两条WAN的此字段不可以填入相同的网址。

4.8 虚拟服务器

在“虚拟服务器”菜单下面，有“虚拟服务器 ”、“UPnP 设置”和“DMZ 主机”三个子项。单击某个子项，您即可进行相应的功能查看与设置。



4.8.1 虚拟服务器

虚拟服务器被定义为一个服务端口，所有外部对此端口的访问将被转向到局域网指定的计算机。



- WAN 口：选择您要设置的 WAN 口数。
- 服务端口段：LAN 端服务端口，即与 WAN 服务端口对接的内网服务端口。

- 内网 IP：输入需要开设虚拟服务的内部主机 IP。
- 协议：选择转发数据的协议类型 TCP/UDP/全部。
- 启用：只有选中该项后本条目所设置的规则才能生效。
- 删除：删除该条规则。

> ⚠*注意：*
> **两个 WAN 口不能配置相同的两条规则。**

例如：您有一台计算机的 IP 地址为 192.168.0.10 的 WEB 服务器，端口为 80；一台计算机的 IP 地址为 192.168.0.11 的 POP3 服务器，端口为 110；一台计算机的 IP 地址为 192.168.0.12 的 FTP 服务器，端口为 21。这时您需要指定如下的虚拟服务器映射表。



> ⚠*注意：*
> **如果设置了服务端口为 80 的虚拟服务器，而且启用了“系统工具”菜单中“远端 WEB 管理”，那么请将“远端 WEB 管理”的端口改为 80 以外的值，如 8080，否则会发生冲突，而导致虚拟服务器不起作用，此功能需要重启路由器才生效。**

4.8.2 UPnP 设置

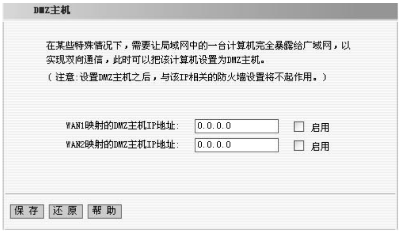
支持最新的 Universal Plug and Play (UPnP 通用即插即用网络协议)，此功能需要 Windows ME/Windows XP 以上的操作系统(注：系统需集成，安装 Directx 9.0 或更新版本)或支持 UPnP 的应用软件才能生效。例如：Windows ME/Windows XP 系统上安装了 MSN Messenger 在音频和视频通话时可以利用 UPNP 协议。启用 UPnP 功能后，当启用相关应用程序后可以看到端口转换信息，端口转换信息由应用程序发出请求时提供。



- ID：表示建立表项的序号。
- 远端主机：接受或发出响应的远端主机的描述。
- 外部端口：端口转换使用的路由器端口号。
- 内部主机：接受或发出响应的内部主机的描述。
- 内部端口：需要进行端口转换的主机端口号。
- 协议：表明是对 TCP 还是 UDP 进行端口转换。
- 持续时间：表明响应的时间段。
- 描述： 映射端口及软件信息。

4.8.3 DMZ 主机

有些程序运行需要多个连接，比如：Internet 游戏、视频会议、Internet 电话等。由于路由器的防火墙的存在，这些程序无法在单纯的虚拟服务下工作。此时可以把该计算机设置成 DMZ 主机。



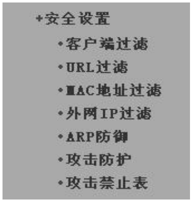
设置步骤：首先在 DMZ 主机 IP 地址输入需设为 DMZ 主机的局域网计算机的 IP 地址，然后点击“启用”完成 DMZ 主机的设置。

⚠*注意：*

设置 DMZ 之后，与该 IP 地址相关的 WAN、LAN 口防火墙将不起作用。

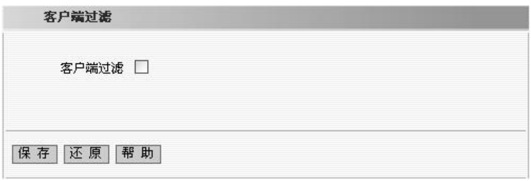
4.9 安全设置

在“安全设置”菜单下面，共有“客户端过滤”、“URL 过滤”、“MAC 地址过滤”、“外网 IP 过滤”、“ARP 防御”、“攻击防护”和“攻击禁止表”七个子项。下面将详细讲解各子项的详细功能。



4.9.1 客户端过滤

为了方便您对局域网中的计算机进行进一步管理,您可以通过数据包过滤功能来控制局域网中计算机对互联网上某些端口的访问。



⚠*注意：*

只有启动“客户端过滤”总开关，其它选项才会显示，已设置的配置文件才会生效。



- 过滤模式：只能选择“禁止”和“允许”中的任何一项，不能混合选择过滤模式。

  禁止：只禁止所设置的规则的数据包禁止通过路由器，其它没有被限制的数据包通过路由器。如选择过滤模式为“禁止”，那么 10 条全部为禁止。

  允许：仅允许所设置的规则的数据包通过路由器，其它数据包全部禁止通过路由器。如选择过滤模式为“允许”，那么 10 条全部为允许。
- 编号：选择您需要设置的编号。
- 启用：选择后该配置文件才生效。
- 注释：即为此配置文件定义的简单描述。
- 局域网 IP 段：填入局域网中被控制的计算机的 IP 地址，您可以使用一个 IP 地址范围。
- 广域网端口：填入预控制的端口，您可以指定一个端口范围，为空表示所有端口 1-65535。
- 类型：选择被控制的数据包所使用的协议（“全部”包括 TCP/UDP）；
- 时间：填入您希望本条规则生效的起始时间和终止时间。如果不设置时间，默认显示为全 0，表示为 24 个小时。

- 日期：根据自身的要求选择相应的选项。
- 保存：完成设置。

例如 1:如果您希望局域网中 IP 地址为 192.168.0.11-192.168.0.22 的计算机在每周的 8:00-18:00 时间段内不能浏览 WEB 网站，对局域网中其它计算机则不做任何限制，这时您需要指定如图的数据包过滤表。



例如 2：如果您希望局域网中 IP 地址为 192.168.0.100-192.168.0.200 的计算机在每周的 8:00-18:00 时间段内允许浏览 WEB 网站，其它局域网中的计算机则不能访问 WEB 网站，这时您需要指定如图的数据包过滤表。



4.9.2 URL 过滤

为了方便您对局域网中的计算机所能访问的网站进行控制,您可以使用域名
过滤功能来指定在什么时段不能访问哪些网站。



⚠ *注意:*

只有启动“URL 过滤”总开关，其它选项才会显示，已设置的配置文件才会生效。



- 过滤模式：只能选择“禁止”和“允许”中的任何一项，不能混合选择过滤模式。

  禁止：只禁止所设置的规则的数据包禁止通过路由器，其它没有被限制的数据包通过路由器。如选择过滤模式为“禁止”，那么 10 条全部为禁止。

允许：只允许该 IP 地址所设置的规则的数据包通过路由器，其它数据包全部禁止通过路由器，其它 IP 地址全部通过路由器。如选择过滤模式为“允许”，那么 10 条全部为允许。

- 编号：选择您需要设置的编号，假如您已经配置好过滤要求，请直接选择配置文件。
- 启用：选择后该配置文件才生效。
- 注释：即为此配置文件定义的简单描述。
- 开始 IP：填入局域网中被控制的计算机的 IP 地址。
- 结束 IP：填入局域网中被控制的计算机的 IP 地址。
- URL 字符串：填入被过滤的域名和域名的一部分。
- 时间：填入您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的选项。
- 保存：完成设置。

例如 1：如果您只希望局域网中 IP 地址为 192.168.0.33~192.168.0.33 的计算机不能浏览包含“sex”字符串的 WEB 网站，其它计算机可以正常浏览包含“sex”字符串的 WEB 网站，您需要指定如图的数据包过滤表。



例如2:如果您只希望局域网中IP地址为192.168.0.2~192.168.0.10的计算机只浏览包含“sina”字符串的WEB网站，则其它计算机可以正常浏览所有的WEB网站，您需要指定如图的数据包过滤表。

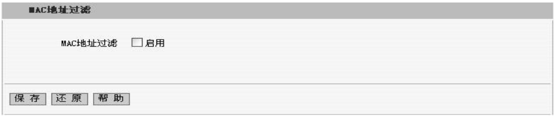


⚠*注意:*

Windows 操作系统有缓存DNS记录的功能，设置完本项后你可能需要重新启动客户端，或在客户端的MSDOS窗口中输入“net stop dnscache”，否则可能会导致可以继续访问过滤掉的网址。

4.9.3 MAC 地址过滤

为了更好的对局域网中的计算机进行管理，您可以通过 MAC 地址过滤功能控制局域网中计算机对 Internet 的访问。



注意：

只有启动“MAC 地址过滤”总开关，其它选项才会显示，已设置的配置文件才会生效。



- ➢ 过滤模式：只能选择“禁止”和“允许”中的任何一项，不能混合选择过滤模式。

  禁止：只禁止所设置的规则的数据包禁止通过路由器，其它没有被限制的数据包通过路由器。

  允许：仅允许所设置的规则的数据包通过路由器，其它数据包全部禁止通过路由器。
- ➢ 注释：即为此配置文件定义的简单描述。
- ➢ MAC:输入您要控制的 MAC 地址或直接选择后面的手动设置中的 MAC 地址。

- 时间：填入您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的选项。
- 保存：完成该设置。
- 删除：删除对应的该条规则。

例如 1：如果您不希望局域网中 MAC 地址为 00:E0:38:03:10:50 的计算机在 8:00-18:00 时间段内不能访问 Internet，而希望局域网中的其它计算机能访问 Internet，这时您需要指定如图的数据包过滤表。



例如 2：如果您只希望局域网中 MAC 地址为 00:00:00:00:00:56 的计算机在 8:00-18:00 时间段内访问 Internet，不希望局域网中的其它计算机访问 Internet，这时您需要指定如图的数据包过滤表。



4.9.4 外网 IP 过滤

为了防止外网的攻击及黑客攻击,当您知道外网的 IP 地址或端口时,您可以在此表中禁止所有数据进入局域网络，保护您的网络。



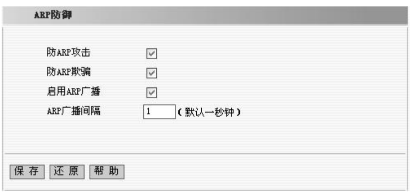
- ID：外网 IP 过滤的编号。
- 外网开始 IP 和结束 IP：输入您要控制的外网的 IP 地址和结束 IP 地址。
- 服务端口段：输入您要控制的外网端口或端口段。
- 启用：启用已设置的规则。
- 删除：删除已设置的规则。
- 协议：默认情况下为全部协议。

例如：希望局域网中的计算机不能访问外网的 IP 地址 58.60.112.222，端口为全部 1-65535，这时您需要指定如图的数据包过滤表。



4.9.5 ARP 防御

为了防止内网发生 ARP 攻击、欺骗，路由器默认开启了此功能，让您的网络更安全。ARP 广播间隔默认为一秒钟，可设置范围为 1-60 秒钟。



4.9.6 攻击防护

攻击防护是路由器防火墙对经过的数据包的检查，以应对一些恶意的攻击。攻击防护分为五类：

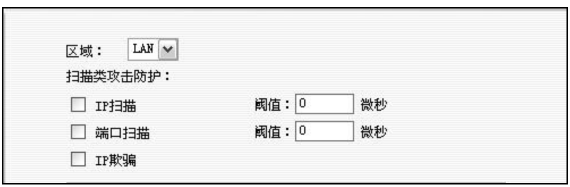
- 扫描类攻击防护
- DoS 类攻击防护
- 可疑包类防护
- 含有 IP 选项的包防护
- 其它防护

4.9.6.1 区域设置

区域设置表明设置的攻击防护对应来自指定区域的数据包进行监控，如选择 WAN 口，则表示对来自局域网的数据包进行监控。

4.9.6.2 扫描类攻击防护

扫描类攻击防护包括三种类型：IP 扫描、端口扫描、IP 欺骗，下面详细介绍各个功能的作用及原理。



4.9.6.2.1 IP 扫描

这是指在小于规定的时间内，一个源 IP 发送 ICMP 请求包到 10 个不同的目的 IP 地址，则被认为此源地址正在进行 IP 扫描攻击。阈值选择范围为 2000-1000000 微秒。

4.9.6.2.2 端口扫描

这是指在小于规定的时间内，一个源 IP 发送 TCP SYN 包到同一目的地址的 10 个不同端口，则被认为此源地址正在进行端口扫描攻击。阈值选择范围为 2000-1000000 微秒。

4.9.6.2.3 IP 欺骗

选中 IP 欺骗复选框，表明检查来自指定区域的包是否正在进行 IP 欺骗。注意：本功能仅在区域为 LAN 时有效，在区域为 WAN 时是无效的。

4.9.6.3 DoS 类攻击防护

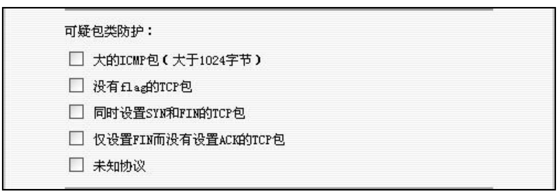
DoS 类攻击防护包括五种类型：ICMP Flood、UDP Flood、SYS Flood、Land、Attack、WinNuke。



- ICMP Flood：这是指在一秒钟内，如果一个目的 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 的攻击。
- UDP Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。
- SYN Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。
- LAND：这是将 SYN Flood 攻击和 IP 欺骗结合在一起的攻击，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 封包，将其作为目的和源 IP 地址时，就发生了 LAND 攻击。
- WinNuke：WinNuke 是针对网上运行 Windows 的任何计算机的 DoS 攻击。攻击者将 TCP 片段(通常给设置了紧急[URG]标志的 NetBIOS 端口 139）发送给具有已建连接的主机。 这样就产生 NetBIOS 碎片重叠，从而导致运行 Windows 的机器崩溃。

4.9.6.4 可疑包类防护

可疑包类防护包括五类：大的 ICMP 包（大于 1024 字节）、没有 flag 的 TCP 包、同时设置 SYN 和 FIN 的 TCP 包、仅设置 FIN 而没有设置 ACK 的 TCP 包、未知协议。

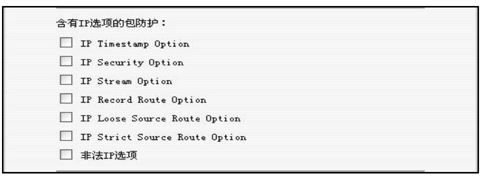


- 大的 ICMP 包：ICMP 包一般不会大于 1024 字节，大于 1024 字节的 ICMP 包则认为是可疑包。
- 没有 flag 的 TCP 包：正常的 TCP 包包头至少设置有一个标志（flag）。未设置任何控制标志的 TCP 包是一个可疑包。
- 同时设置 SYN 和 FIN 的 TCP 包：在同一 TCP 片段包头中同时设置 SYN 和 FIN 控制标志是异常的 TCP 包。
- 设置 FIN 未设置 ACK 的 TCP 包：设置了 FIN 标志，而未设置 ACK 标志的 TCP 包是异常的 TCP 包。
- 未知协议：IP 包头中协议类型字段的 135 或更大值为保留的，尚未定义。 正是由于这些协议未定义，就无法事先知道某一特定的未知协议是善意的还是恶意的。对这些非标准协议，谨慎的态度是封锁这类未知的元素进入受防护网络。

4.9.6.5 含有 IP 选项的包防护

对最常用的通信这些选项是不必要的，在实际的使用中，它们也很少出现在 IP 包头中，这些选项经常被用与某些恶意用途。

IP 选项包括：IP Timestamp Option、IP Security Option、IP Stream Option、IP Record Route Option、IP Loose Source Route Option、IP Strict Source Route Option、非法 IP 选项。

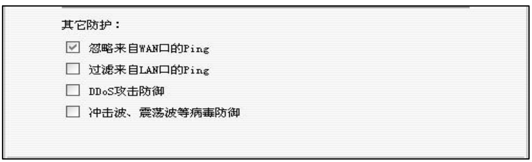


- IP Timestamp Option：表明是否检查来自指定区域的 IP 包含有

Internet Timestamp 项。

- IP Security Option：表明是否检查来自指定区域的 IP 包含有 Security 项。
- IP Stream Option:表明是否检查来自指定区域的 IP 包含有 Stream ID 项。
- IP Record Route Option：表明是否检查来自指定区域的 IP 包含有 Record Route 项。
- IP Loose Source Route Option：表明是否检查来自指定区域的 IP 包含有 Loose Source Route 项。
- IP Strict Source Route Option：表明是否检查来自指定区域的 IP 包含有 Strict Source Route 项。
- 非法 IP 选项:表明是否检查来自指定区域的 IP 包的完整性或正确性。

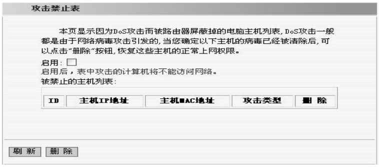
4.9.6.6 其它防护



- 忽略来自 WAN 口的 Ping：忽略来自 WAN 口的 Ping。
- 过滤来自 LAN 口的 Ping：启用可防冲击波病毒攻击。
- 路由器可以防御 DDos 攻击、冲击波、震荡波等病毒。

4.9.7 攻击禁止表

本页显示因为 DoS 攻击而被路由器屏蔽掉的电脑主机列表，DoS 攻击一般都是由于网络病毒攻击引发的，当您确定以下主机的病毒已经被清除后，可以点击“删除”按钮，恢复这些主机的正常上网权限。



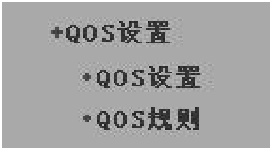
- 启用：默认为关闭，启用后，表中攻击的计算机将不能访问网络。
- 此功能只有开启防火墙的“扫描类攻击防护”“DoS 类攻击防护”和“DDoS 攻击防御”后才会生效。
- 路由器一旦发现有电脑存在病毒或制造恶意攻击，自动将其 IP 地址和 MAC 地址显示在列表中，如果您开启了此功能，那么该表中的计算机将其无法正常上网。

例如：此功能启用，攻击的计算机信息显示在列表中，当您确定列表中的计算机已经清除病毒或删除了恶意攻击程序，可以将列表删除，恢复被禁止电脑的正常上网功能，如下表：



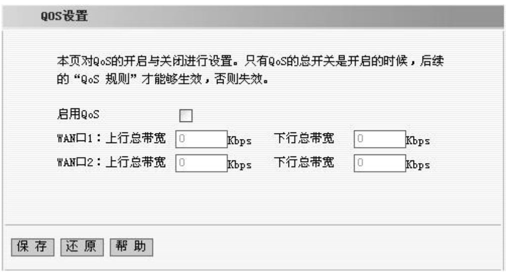
4.10 Qos 设置

在“Qos 设置”菜单下面，有“Qos 设置”和“Qos 规则”二个子项。单击某个子项，您即可进行相应的功能查看与设置。



4.10.1 Qos 设置

本页对 Qos 的开启和关闭进行设置。只有 Qos 启用时，后面的“Qos 规则”才能生效；运行状态中的“带宽利用率”才能生效。



- 启用 Qos：开启后，Qos 规则和带宽利用率将起作用。
- 上行总带宽：填写 ISP 实际给您分配的上行速度值。
- 下行总带宽：填写 ISP 实际给您分配的下行速度值。
- 单位：如果 ISP 给您分配的带宽为：上行 0.5M、下行 2M，单位进行换算后，您应该填入上行 512 Kb/s、下行 2048Kb/s。

⚠*注意：*

如果 WAN 口上下行总带宽值填入不准确，会影响 Qos 规则和带宽利用率的准确性，不清楚可咨询 ISP 服务商。

4.10.2 Qos 规则

Qos 规则分为 Qos 规则列表和 Qos 规则配置。

4.10.2.1 Qos 规则列表

在 Qos 规则列表中，可以查看用户创建的全部规则，每个规则的条目有：

- ID：表示是的第几条规则。
- 描述：此规则的备注信息。
- IP 段：局域网中要控制的计算机的 IP 地址。
- 协议：有全部、TCP、UDP 三个选项。
- 端口段：输入您要控制的端口号或端口段。
- 模式：可分为独立带宽和共享带宽：独立带宽表示地址或端口各自拥有单独的上下行带宽值；共享带宽表示地址或端口共享上下行带宽值。
- 上行带宽：通过 WAN 口允许的最大上传速度限制和最小上传速度限制。为 0 表示采用缺省值。
- 下行带宽：通过 WAN 口允许的最大下传速度限制和最小下传速度限制。为 0 表示采用缺省值。
- 启用：规则的状态。
- 配置：可对规则进行编辑及删除处理。

4.10.2.2 Qos 规则配置

在 Qos 规则配置中，可以创建新规则或修改已存在的规则。您需要设置的条目如下：



- 启用：此条规则是否生效。
- 描述：此规则的备注信息。
- 地址段：局域网中要控制的计算机的 IP 地址。
- 端口段：输入您要控制的端口号或端口段。
- 协议：有全部、TCP、UDP 三个选项。
- 模式：可分为独立带宽和共享带宽：独立带宽表示地址或端口各自拥有单独的上下行带宽值；共享带宽表示地址或端口共享上下行带宽值。
- 上行带宽：通过 WAN 口允许的最大上传速度限制和最小上传速度限制。为 0 表示采用缺省值。
- 下行带宽：通过 WAN 口允许的最大下传速度限制和最小下传速度限制。为 0 表示采用缺省值。
- 保存：保存此规则的配置信息。

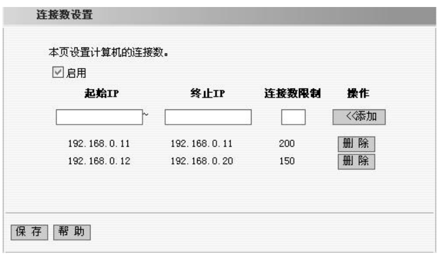
4.11 连接数设置

本页设置单机的连接数限制。对指定 IP 地址的计算机连接数进行限制，超过限制的新连接不允许通过路由器，未指定的计算机可以不受限制的建立连接。



- 启用：启用连接数限制功能。
- 起始终止 IP：输入要控制的计算机的 IP 地址段，也可以直接单个 IP 地址。
- 连接数限制：该计算机允许的最大连接数。
- 操作：将此规则添加到连接数表中。

例如：您希望限制的计算机的 IP 地址为 192.168.0.11-192.168.0.11，允许的最大连接为 200；计算机的 IP 地址为 192.168.0.12-192.168.0.20，允许的最大连接为 150；这时您需要做如图配置。



4.12 IP 与 MAC 绑定

本页设置单机的 MAC 地址和 IP 地址的匹配规则，防止其他非法 IP 和非法 MAC 接入网络，防止 ARP 欺骗。

IP 与 MAC 绑定是指定的 IP 地址的主机，在向路由器发送 ARP 请求时，其 MAC 地址必须和 IP 地址相同，允许通过路由器；否则为非法，并不允许使用该 IP 地址的主机的 ARP 请求通过路由器。



- 全部导入：只是导入“流量统计”页面中显示的 IP 和 MAC 地址，如网内需增加 IP 和 MAC 地址，需手动进行添加。
- ARP 绑定：是否开启 IP 与 MAC 绑定功能。如开启后，只有 IP 和 MAC 绑定表中存在的 IP 和 MAC 地址才可以访问网络。
- 增加单个条目：在静态列表添加新的条目。
- 使能所有条目：使当前静态列表中所有条目的绑定生效。
- 删除所有条目：删除静态列表表中所有条目。
- 查找指定条目：在静态列表中查找 IP 和 MAC 地址的条目。

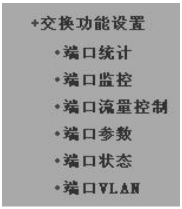
4.13 流量统计



- 启用统计：系统默认为开启，统计局域网中的计算机的流量和连接数。如不需流量统计，可关闭此功能，可提高路由器的数据包处理能力。
- 每 5 秒自动刷新：如开启此功能，每过 5 秒钟自己动刷新页面，同时自动更新各计算机的流量值。
- 排序：表中的数据按照您选择的规律进行排列，分为：按 IP 地址排序、按总流量 TX 包数排序、按总流量 TX 字节排序、按总流量 RX 包数排序、按总流量 RX 字节排序、按 TX 速率排序、按 RX 速率排序、按连接数排序。
- IP 地址：被统计计算机的 IP 地址。
- MAC 地址：被统计计算机的 MAC 地址。
- 总流量：数据包数-路由器总的收、发数据的包的个数；字节数-路由器总的收、发数据的字节数。
- 速率：路由器当前 1 秒钟收、发数据的速度。
- 连接数：当前统计的计算机已使用的连接数。
- 限制：此 IP 地址禁止访问网络。
- 导入：将此条目导入“IP 与 MAC 绑定”表中。

4.14 交换功能设置

在“交换功能设置”菜单下面，共有“端口统计”、“端口监控”、“端口流量控制”、“端口参数”、“端口状态”、“端口 VLAN” 六个子项。单击某个子项，您即可进行相应的功能设置或相关的状态，下面将详细讲解各子项的功能。



4.14.1 端口统计

端口统计将针对每一个端口，统计它收发多少数据字节、多少数据帧、多少个广播帧、多少个错误帧等等。



Rx Unicasts：	335570	Tx Unicasts：	365312
Rx Broadcasts：	158261	Tx Broadcasts：	102141
Rx Multicasts：	2406	Tx Multicasts：	17
Rx Bytes：	60804151	Tx Bytes：	261982301
Rx Pauses：	0	Tx Pauses：	0
Rx CRC Errors：	0	Collisions：	0
64 B：	119732	65to127 B：	56748
128to255 B：	24297	256to511 B：	75416
512to1023 B：	68957	1024toMax B：	122320
RX Undersizes：	0	RX Fragments：	0
RX Oversizes：	0	RX Jabbers：	0

- Rx Unicasts：接收的数据帧的目的 MAC 地址为单播 MAC 地址的数据帧数目。
- Tx Unicasts：发送的数据帧的目的 MAC 地址为单播 MAC 地址的数据帧数目。
- Rx Broadcasts：接收的数据帧的目的 MAC 地址为广播 MAC 地址的数据帧数目。
- Tx Broadcasts：发送的数据帧的目的 MAC 地址为广播 MAC 地址的数据帧数目。
- Rx Multicasts：接收的数据帧的目的 MAC 地址为多播 MAC 地址的数据帧数目。
- Tx Multicasts：发送的数据帧的目的 MAC 地址为多播 MAC 地址的数据帧数目。
- Rx Bytes：接收的数据帧的总字节数（不包括错误帧）。
- Tx Bytes：发送的数据帧的总字节数（不包括错误帧）
- Rx Pauses：接收的 Pause 的数据帧数目。
- Tx Pauses：发送的 Pause 的数据帧数目。
- Rx CRC Errors：接收的含非法效验字段的数据帧数目。
- Rx Collisions：接收数据帧时产生的冲突数目。
- 64 B：接收及转发的长度为 64 字节的数据帧数目（包含错误帧）。
- 65to127 B：接收及转发的长度为 65～127 字节的数据帧数目（包含错误帧）。
- 128to255 B：接收及转发的长度为 128～255 字节的数据帧数目（包含错误帧）。
- 256to511 B：接收及转发的长度为 256～511 字节的数据帧数目（包含错误帧）。
- 512to1023 B：接收及转发的长度为 512～1023 字节的数据帧数目

（包含错误帧）。

- 1024toMax：收及转发的长度为 1024～1518 字节的数据帧数目（包含错误帧）。
- Rx Undersizes：接收的长度小于 64 字节并且包含合法校验字段的数据帧数目。
- Rx Fragments：接收的长度小于 64 字节并且包含非法校验字段的数据帧数目。
- Rx Oversizes：接收的长度超过最大字节数并且包含合法校验字段的数据帧数目。
- Rx Jabbers：接收的长度超过最大字节数并且包含非法校验字段的数据帧数目。

4.14.2 端口监控

本页设置端口监控功能的基本参数，端口监控主要是使用一个监控端口对一个或多个被监控端口进行输出监控或输入输出监控。此处说的输入输出是相对交换机而言。



- 监控设置：包括禁用、输出监控和输入输出监控。这里的输入输出是相对路由器交换机部分而言。
- 监控端口：连接监控主机的端口。

- 被监控端口：可选择 1 到 4 个端口为被监控端口。
- 注意：监控端口不支持跨 VLAN 的监控，当设置多个 VLAN 时，请注意将监控端口添加到要监控的端口成员所在的 VLAN 上。

4.14.3 端口流量控制

端口流量控制提供针对每个端口的流量进行设置，入口限制模式提供“不限制”、“FLOOD”、“广播和多播”、“广播”、“所有帧”等五种不同的控制模式，而出口控制则是针对所有帧的控制。



- 不限制：不进行限制。
- FLOOD：对广播、多播帧、以及帧的目的 MAC 地址不存在于地址表的帧进行控制。
- 广播和多播：对广播和多播帧进行控制。
- 广播：对广播帧进行控制。
- 所有帧：现在所有的帧。

其中 FLOOD 、广播、多播和广播的限制方式就是管理型交换机中的广播风暴抑制，路由器中的交换机部分可以对三种广播帧（广播包、组播包、未学习到地址的单播包）进行过滤。

一个数据帧或包被传输到本地网段 (由广播域定义)上的每个节点就是广播；由于网络拓扑的设计和连接问题，或其他原因导致广播在网段内

大量复制，传播，导致网络性能下降，甚至网络瘫痪。这就是广播风暴。

当设置所有帧的限制方式时，交换机部分对所有的数据帧都进行控制，对于入口的数据包采用过滤处理，当前流量超出入口限制流量时，超出部分会被丢弃；对于出口的数据，仅限制流量（根据端口流量控制的开启情况决定是否丢弃超出限制速率外的帧），这时起到端口下行带宽限制的作用。

4.14.4 端口参数

本页主要包括：是否使能端口、是否启用流量控制以及设置工作模式。



- 端口的工作模式

  共四种模式 10M 半双工、10M 全双工、100M 半双工、100M 全双工、自协商。

  如 100M 全双工，前面的数字表示的是传输速率，后面表示的是双工模式。所谓半双工就是传输的两边既可以发送，也可以接收，但是在某一时刻只能有一个设备使用网络传输介质，即不能同时进行发送和接收；所谓全双工是传输的两边可以同时的发送和接收，相互不影响。

- 端口自动协商功能

  该交换机的端口可根据另一端口设备的速度和双工模式，自动

调节速度和双工模式到双方都可以达到的最高水平,并实现自动调整传输方式（全双工和半双工）和传输模式（10Mbps、100Mbps）的功能。

➢ 流量控制

流量控制是为了同步接收放和发送方的速度而进行的控制。当接收方接收能力比发送方能力小的时候,如果没有流量控制就会丢失数据。流量控制主要分两种情况：全双工下和半双工下。

全双工：当数据的发送和接收分流，分别由两根不同的传输线传送时，通信双方都能在同一时刻进行发送和接收操作，这样的传送方式就是全双工制，在全双工方式下，通信系统的每一端都设置了发送器和接收器，因此，能控制数据同时在两个方向上传送。全双工方式无需进行方向的切换，因此，没有切换操作所产生的时间延迟，这对那些不能有时间延误的交互式应用（例如远程监测和控制系统）十分有利。这种方式要求通讯双方均有发送器和接收器，同时，需要 2 根数据线传送数据信号。

半双工：当接收设备的资源不足时就会启用流量控制，由于发送方发送时接收方可以发送数据给发送方，接收方通过发送一个 PAUSE 帧告诉发送方停止一段时间后再发送数据。这就是全双工下的流量控制 IEEE802.3X 标准。

4.14.5 端口状态

端口状态标识端口上是否接有设备,如果接有设备就会知道它的工作速率是多少、工作模式、是否开启了流控等。


端口状态

端口	端口状态	连接速率(Mbps)	双工模式	流量控制
1	已连接	100	全双工	启用
2	已连接	100	全双工	启用
3	已连接	100	全双工	启用

刷 新

4.14.6 端口 VLAN

VLAN 是英文 Virtual Local Area Network 的缩写，中文名为"虚拟局域网"， VLAN 是一种将局域网（LAN）设备从逻辑上划分（注意，不是从物理上划分）成一个个网段（或者说是更小的局域网 LAN)，从而实现虚拟工作组（单元）的数据交换技术。

VLAN 的好处主要有三个：

- 端口的分隔。即便在同一个交换机上，处于不同 VLAN 的端口也是不能通信的。这样一个物理的交换机可以当作多个逻辑的交换机使用。
- 网络的安全。不同 VLAN 不能直接通信，杜绝了广播信息的不安全性。
- 灵活的管理。更改用户所属的网络不必换端口和连线，只更改软件配置就可以了。

VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。 VLAN 除了能将网络划分为多个广播域，从而有效地控制广播风暴的发生，以及使网络的拓扑结构变得非常灵活的优点外，还可以用于控制网络中不同部门、不同站点之间的互相访问。

本路由器支持基于端口的 VLAN。

这是最常应用的一种 VLAN 划分方法，应用也最为广泛、最有效，目前绝大多数 VLAN 协议的交换机都提供这种 VLAN 配置方法。这种划分 VLAN 的方法是根据以太网交换机的交换端口来划分的，它是将 VLAN 交换机上的物理端口，每个组构成一个虚拟网，相当于一个独立的 VLAN 交换机。

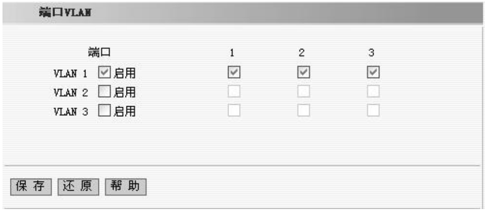
对于不同部门需要互访时，可通过路由器转发，并配合基于 MAC 地址的端口过滤。对某站点的访问路径上最靠近该站点的交换机、路由交换机或路由器的相应端口上，设定可通过的 MAC 地址集。这样就可以防止非法入侵者从内部盗用 IP 地址从其他可接入点入侵的可能。

从这种划分方法本身我们可以看出，这种划分的方法的优点是定义 VLAN 成员时非常简单，只要将所有的端口都定义为相应的 VLAN 组即可。适合于任何大小的网络。它的缺点是如果某用户离开了原来的端口，到了一个新的交换机的某个端口，必须重新定义。

设置 VLAN 时请遵循以下几条规则：

- 已启用的 VLAN 不允许存在 VLAN 包含的关系。
- 已启用的 VLAN 的端口成员不允许为空，允许单独一个端口构成一个 VLAN。

- 当前启用的 VLAN 条目不允许为空。

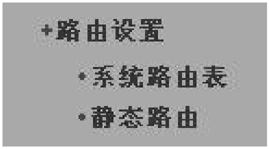


注意：

当一个端口不属于任何 VLAN 时，它和单独构成一个 VLAN 时一致。

4.15 路由设置

在“路由设置”菜单下面，共有“路由表”和“静态路由”两个子项。，下面将详细讲解各子项的详细功能。



4.15.1 系统路由表

本页显示路由器核心路由表的内容。



系统路由表

目的IP	子网掩码	网关	metric	接口
0.0.0.0	0.0.0.0	219.133.207.1	0	ixe1
192.168.0.0	255.255.255.0	192.168.0.1	0	ixe0
219.134.150.110	255.255.255.255	219.134.150.110	0	ixe1

刷新

4.15.2 静态路由

本页设置路由器的静态路由功能，您可以指定静态路由规则。



- 目的网络 IP：目的主机的 IP 地址或目的网络的 IP 地址。
- 子网掩码：目的地址的子网掩码，一般为 255.255.255.0。
- 网关：下一跳路由器入口的 IP 地址。
- 添加：将此条目添加中表中。

⚠*注意：*

网关 IP 必须是与 WAN 或 LAN 口属于同一个网段。

目的 IP 地址如果是一台主机 IP 地址,子网掩码须为 255.255.255.255。

目的 IP 地址如果为 IP 网段，则须与子网掩码匹配。例如，如果目的 IP 为 10.0.0.0，子网掩码须为 255.0.0.0；如果目的 IP 为 10.1.2.0，子网掩码须为 255.255.255.0。

4.16 动态 DNS

4.16.1 花生壳

本页设置“花生壳”的 DDNS 参数，当连接状态显示成功之后，互联网上的其它主机可以通过以域名的方式对您的路由器或虚拟服务器进行访问了。



- DDNS 服务：DDNS 总开关，只有开启后，下面的功能才会生效。
- 服务提供商：选择提供 DDNS 的厂家。
- 用户名：在 DDNS 服务器上注册的用户名。
- 密码：在 DDNS 服务器上注册的密码。
- 域名信息：当前从 DDNS 服务器获得的域名，也可手动输入。
- 连接状态：当前从 DDNS 服务器的连接状态。

4.16.2 88IP

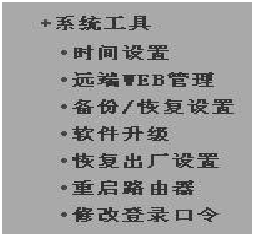
本页设置“88IP”的 DDNS 参数，当连接状态显示成功之后，互联网上的其它主机可以通过以域名的方式对您的路由器或虚拟服务器进行访问了。



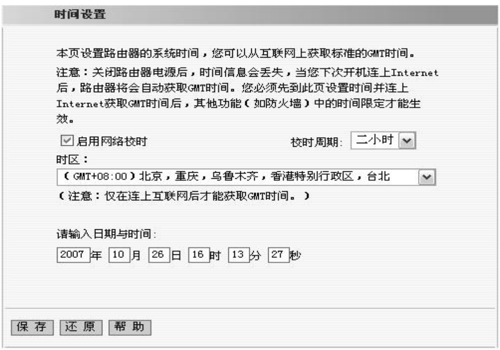
- DDNS 服务：DDNS 总开关，只有开启后，下面的功能才会生效。
- 服务提供商：选择提供 DDNS 的厂家。
- 用户名：在 DDNS 服务器上注册的用户名。
- 密码：在 DDNS 服务器上注册的密码。
- 域名信息：当前从 DDNS 服务器获得的域名，也可手动输入。
- 连接状态：当前从 DDNS 服务器的连接状态。

4.17 系统工具

在“系统工具”菜单下面，共有“时间设置”、“远程 WEB 管理”、“备份/恢复设置”、“软件升级”、“恢复出厂设置”、“重启路由器”“修改登录口令”七个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。



4.17.1 时间设置



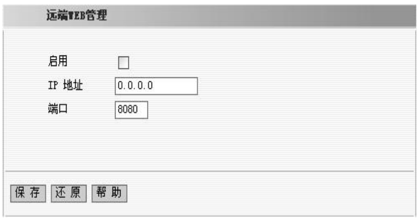
您可以选择自己设置时区从互联网上获取标准的 GMT 时间。当连上互联网后才能获取 GMT 时间，您也可以手动输入当前的时间。

- 启用网络校时：系统时间从网络上自动获取。

- 校时周期：系统时间从网络校时周期，请根据您的需要进行选择，系统默认校时周期为二个小时。
- 时区：选择您当地的时区。

4.17.2 远端 WEB 管理

通常来讲，只有局域网内的用户才能管理路由器。假如有特殊需要，这个功能将使您能在远程管理路由器。



注意：

路由器默认的远程管理可以根据需求进行修改，您必须用“IP 地址：端口”的方式（例如 http://192.168.0.1:8080）才能登录路由器执行远程管理。

路由器默认的远端 WEB 管理 IP 地址为 0.0.0.0，当启用时，广域网中所有计算机都能登录路由器执行远端 WEB 管理，如果您改变了默认的 IP 地址（例如改为 58.60.111.221），则广域网中只有具有指定 IP 地址（例如 58.60.111.221）的计算机才能登录到路由器管理页面。

4.17.3 备份/恢复设置

在这里您可以备份当前或恢复以前的路由器设置。



备份/恢复设置步骤：

- 登录我们公司的网站（www.tenda.com.cn），下载一个 TFTP Server 应用程序，将此程序放到一个固定的目录中并运行。
- 单击“备份”便可以在 TFTP 应用程序的目录生成一个系统配置的备份文件。
- 同样道理，我们只需要把需要上传的系统配置文件放置到 TFTP 的目录中，点击“恢复”，重新启动路由器后将可以恢复到以前的系统配置。

4.17.4 软件升级

通过升级本路由器的软件,您将获得更加稳定的路由器版本及增值的路由功能。



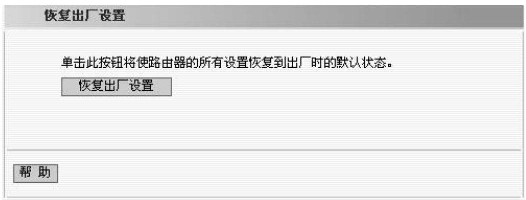
软件升级步骤：

- 登录我们公司的网站（www.tenda.com.cn），下载更高版本的软件。
- 在您局域网中的计算机上开启一个 TFTP Server，并把下载的文件使用 WinRAR 软件解压后置于该 TFTP 服务器的目录中。
- 单击“升级”进行软件升级。
- 升级完成后，路由器将自动重新启动。

⚠*注意：*

升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级成功后，路由器将自动重启。升级过程约数分钟，请等候。

4.17.5 恢复出厂设置



“恢复出厂设置”按钮将使路由器的所有设置恢复到出厂时的默认状态。其中：

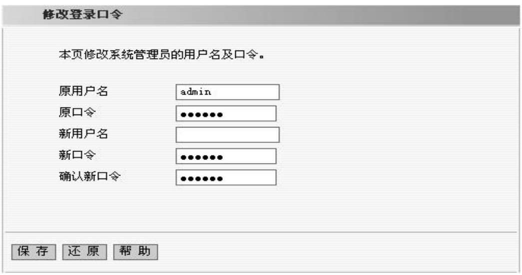
- 默认的用户名为：admin。
- 默认的密码为：admin。
- 默认的 IP 地址为：192.168.0.1。
- 默认的子网掩码为：255.255.255.0。
- 恢复出厂设置后，路由器重新启动才能生效。

4.17.6 重启路由器



“重启路由器”选项将使一些需要重新启动路由才能生效的设置生效。路由器在重启前，会自动断掉网络连接。

4.17.7 修改登录口令



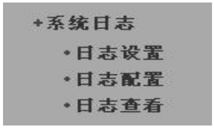
- 本页修改系统管理员的用户名和口令。
- 请您首先输入新的用户名和原来的登陆口令，然后输入您希望使用的新的口令 ，如果您原来的用户口令输入无误的话，单击“保存”即可成功修改系统的用户名和口令。

⚠*注意：*

出于安全考虑，我们强烈推荐您改变初始系统员用户名和密码。

4.18 系统日志

在“系统日志”菜单下面，共有“日志设置”、“日志配置”、“日志查看”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。



4.18.1 日志设置

本页设置 Syslog 服务，目的是将系统产生的日志发送到指定的计算机 Syslog 服务器上，方便用户查看系统的每一个信息。

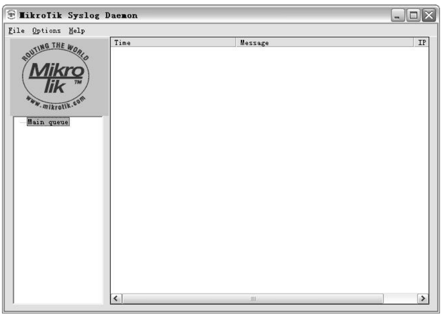


- 启用 Syslog：选择是否启用 Syslog 服务。
- 启用：选择是否启用本 Syslog 服务器。
- 主机 IP 地址：Syslog 服务器的 IP 地址。
- 端口：Syslog 服务的协议端口（默认值为 514），可根据 Syslog 服务器设定的端口进行修改，它应与 Syslog 服务器保持一致。

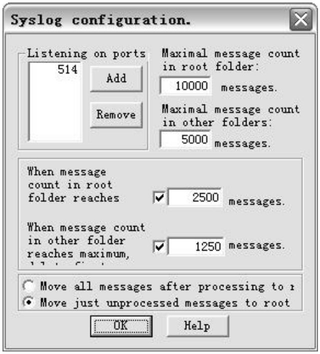
例如：Syslog 服务器请到我公司网站(www.tenda.com.cn)进行下载，局域网计算机的 IP 地址为 192.168.0.10,Syslog 服务器的端口号为 514，那么路由器应该做如下操作。



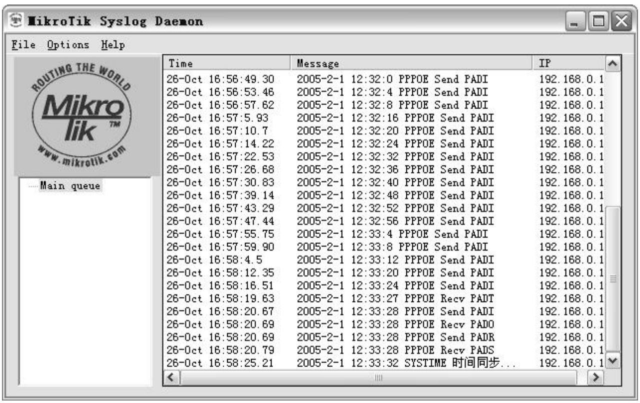
- 计算机的配置：
- 将计算机的 IP 地址改为 192.168.0.10；
- 运行 Syslog 软件；
- 下面将介绍 Syslog 软件的安装及设置；



- 点击菜单“Options”中“configuration”，添加 Syslog 服务器端口 514，并点击保存。



- 当设置完成后，系统日志中的所有信息将会发送到 Syslog 服务器上。



- 时间：表示 Syslog 服务器的系统时间。
- 信息：路由器系统日志中显示的信息。
- IP：路由器的 IP 地址。

4.18.2 日志配置

本页设置系统日志的显示范围，默认情况下，只显示了系统的一般设置，如需要显示更多信息，请启用您需要的选项。



4.18.3 日志查看

- 在系统日志里，您可以查看系统启动出现的各种情况，也可以查看有无网络攻击发生。
- 清除日志：清除系统日志。



4.19 退出登录

各项设置完成后请从“退出登录”安全的完全退出路由器的 WEB 管理页面。

附录一 TCP/IP 地址设置方法（以 WinXP 为例）

依次点击“开始—控制面板”，打开控制面板。（如图 1）。



图 1

单击“网络和 Internet 连接”，进入网络和 Internet 连接页面（如图 2）。



图 2

单击“网络连接”，进入网络连接页面（如图 3）。



图 3

选择“本地连接”，点击鼠标右键，选择“属性”，弹出“本地连接属性”对话框，在“此连接使用下列项目”中选择“Internet 协议（TCP/IP）”，点击“属性”（如图 4）。



图 4

方法 1：选择“自动获得 IP 地址”“自动获得 DNS 服务器地址” 点击“确定”（如图 5）。

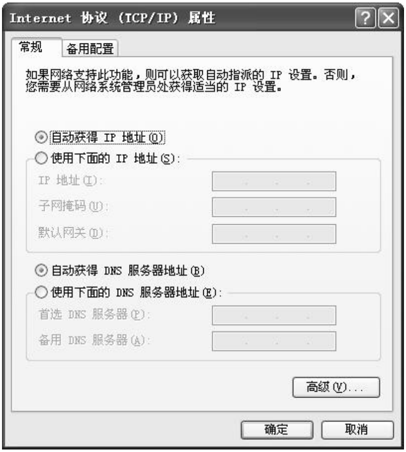


图 5

方法 2:选择“使用下面的 IP 地址”,填写 IP 地址为:192.168.0.xxx.（xxx 为 2~254 中除了 1 的任意数值），子网掩码为 255.255.255.0，网关 192.168.0.1，首选 DNS 服务器：192.168.0.1，如果您知道当地 DNS 服务器地址可直接输入（如图 6）。

点击“确定”回到“本地连接 属性”对话框。

再点击“确定”退出设置界面。

在这一节中，我们介绍一下如何为您的个人计算机配置 TCP/IP 协议。请您确认已经在您的计算机中成功安装了网卡，如果没有，请参阅网卡的用户手册，正确安装网卡硬件及驱动程序。

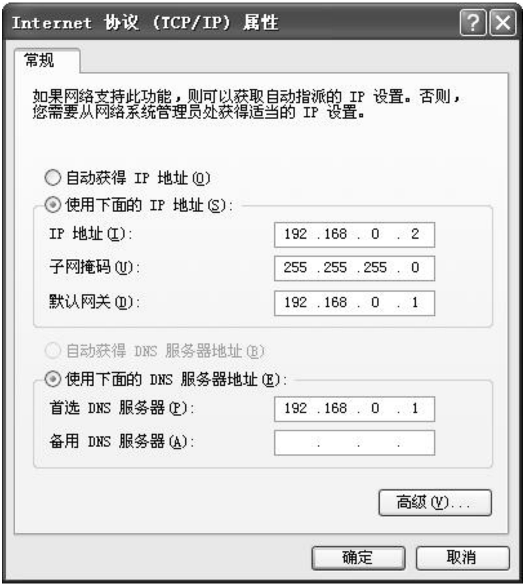


图 6

附录二：常用命令介绍

常用命令	命令说明
Cmd	运行此命令可快速进入 Windows 的命令行模式（适用与 Windows2000 以上操作系统）
Ipconfig	显示本机 IP 地址，如 ipconfig /all 查看
Ping	这是 TCP／IP 协议中最有用的命令之一，它给另一个系统发送一系列的数据包，该系统本身又发回一个响应，这条实用程序对查找远程主机很有用，它返回的结果表示是否能到达主机，宿主机发送一个返回数据包需要多长时间。
Netstat	能检验 IP 的当前连接状态，在断定您的基本通信正在进行后，就要验证系统上的服务。这个服务包括检查正在收听输入的通信量和／或验证您正在创建一个与远程站点的会话，它可以很轻松地做到这一点。
tracert	Tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能同 Ping 类似，但它所获得的信息要比 Ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。
net stop	停止 Windows NT 网络服务， 如：net stop dnscache
net send	向网络的其他用户、计算机或通信名发送消息。要接收消息必须运行信使服务。